Reconocimiento biométrico en aplicaciones de E-Government. Análisis de confiabilidad / tiempo de respuesta.

José I. Carri [1], Ariel Pasini [2], Patricia Pesado [3], Armando De Giusti [4]
{jicarri,apasini,ppesado,degiusti}@lidi.info.unlp.edu.ar

Instituto de Investigación en Informática LIDI (III-LIDI)
Facultad de Informática – UNLP

Abstract

An analysis of the use of biometric recognition in E-Government applications is presented.
In particular, this paper discusses the use of digital fingerprints, analyzing the recognition time and the system reliability in function of the increasing number of users.
The systematic study of the recognition response in function of the DB size is presented together with an analysis of the recognition reliability, considering the information loss levels in the digitalization -"scanning"- of the user's fingerprints.
Finally, previous studies are composed with the requirements of an Internet-based WEB service to analyze a projection of the attainable response times with different numbers of users.

Keywords: *E-Government, Biometric Recognition, Fingerprints, Reliability.*

Resumen

Se presenta un análisis de la utilización de reconocimiento biométrico en aplicaciones de E-Government.
En particular se discute el empleo de huellas digitales, analizando el tiempo de reconocimiento y la confiabilidad de los sistemas utilizados en función de un número creciente de usuarios.
Se presenta un estudio sistemático del tiempo de respuesta del reconocimiento en función del tamaño de la BD y asimismo un análisis de la confiabilidad del reconocimiento, considerando niveles de pérdida de información en la digitalización ("scanning") de la huella del usuario.
Por último se componen los estudios anteriores con los requerimientos de un servicio WEB basado en Internet, para analizar una proyección de los tiempos de respuesta alcanzables con diferente número de usuarios.

Palabras Clave: *Gobierno electrónico, reconocimiento biométrico, huellas digitales, confiabilidad.*

VI Workshop de Ingeniería de Software y Bases de Datos

[1] Becario III-LIDI. Facultad de Informática UNLP.
[2] Jefe de Trabajos Prácticos. Facultad de Informática. UNLP.
[3] Profesor Titular. Facultad de Informática UNLP/ Profesional CIC.
[4] Investigador Principal CONICET. Profesor Titular D.E. Facultad de Informática UNLP.

1. Introducción

En la actualidad el problema de la identificación personal se ha convertido en un desafío para los sistemas de seguridad, por el desarrollo mismo de la tecnología y sus aplicaciones "a distancia" tales como E-Government, E-Commerce o E-Learning [1], [2], [3].

Tecnologías como las tarjetas de ingreso, las tarjetas bancarias, las claves de acceso vía InterNet o cualquier combinación de usuario-password presentan puntos débiles en la seguridad, que pueden resultar críticos según la clase de aplicación en la que estén involucradas [4]. De hecho la identificación fehaciente de la persona en tiempo real es un objetivo complejo al que se enfoca el reconocimiento biométrico [5].

Las técnicas biométricas utilizan características fisiológicas o de comportamiento de las personas para identificarlas: las técnicas de reconocimiento de rostro, de huellas dactilares, de iris, de retina y de la geometría de la mano son las más reconocidas para analizar las características fisiológicas [6], mientras que el reconocimiento de firma y el reconocimiento de voz son las más utilizadas para analizar características de comportamiento [7].

Un sistema biométrico puede ser utilizado para verificación o identificación de una persona. En el caso de verificación se lo utiliza para certificar su identidad: la persona debe primero identificarse con algún otro método y luego se verifica la identidad con una técnica biométrica [16].
En el caso de la identificación, directamente el sistema indica cual es la identidad de la persona. Cada técnica tiene sus características particulares, pero todas tienen dos etapas: registro y verificación o identificación.
El registro en el sistema es el entrenamiento para identificar a una persona. En principio la persona provee su identificación, con algún tipo de documentación, y luego se expone a un dispositivo de adquisición de características (dependiendo de la tecnología utilizada), luego esa información se codifica, se asocia a la identidad de la persona y se almacena. El proceso de registro es muy importante ya que de ese momento en adelante las características físicas de la persona quedarán asociadas a la identidad de la misma.
La etapa de verificación consiste en identificar a una persona que ya se encuentra registrada y validar su identificación adquiriendo las características biométricas y comparándolas con las almacenadas en el sistema.
En este caso la comparación de las características se realiza de una contra una. En la identificación, el sistema directamente adquiere las características biométricas y compara contra toda la base en busca de un patrón que coincida con el adquirido.

A continuación se da una breve definición de las diferentes técnicas biométricas:

Reconocimiento de rostro:
Identifica a las personas a través de los rasgos faciales, tratando de copiar el comportamiento de los humanos al identificar la imagen de un rostro dentro de un conjunto de imágenes preestablecido [8]. Nos permite poder identificar a una persona sin interferir en sus actividades. Es decir no sólo nos permite verificar la identidad de una persona con el consentimiento de la misma, sino que podemos identificarla sin contacto físico.
La técnica tiene un espectro amplio de aplicaciones tanto para verificación como para identificación, pero principalmente son utilizadas en sistemas de vigilancia y seguridad.

Reconocimiento de iris:

Se basa en el color de los distintos anillos que rodean la pupila del ojo.
El iris es una fuente muy importante de características biométricas, ya que tiene aproximadamente 266 características distintas, las cuales se forman en el octavo mes de gestación y permanecen inalterables a lo largo de toda la vida de la persona.
Este reconocimiento se puede aplicar tanto para verificación como para identificación.
Tanto en el proceso de registro como el de identificación se debe contar con la colaboración de la persona ya que se trata de un proceso invasivo que consiste en escanear el ojo con un dispositivo de alta calidad y luego armar un sistema de coordenadas con las características del iris.
Se trata de una tecnología de alto costo, con la que se desarrollan sistemas utilizados para acceder a lugares de alta seguridad [9].

Reconocimiento de retina:
Consiste en capturar y analizar los patrones de las venas de la parte trasera del globo ocular.
El patrón ocular es único de cada persona, y son normalmente estables a lo largo de la vida aunque enfermedades como diabetes, glaucoma o presión alta pueden modificarlo.
El proceso de registro e identificación se realiza con dispositivos muy complejos que requieren que la persona adopte posiciones especiales, lo cual hace que sea la técnica biométrica más invasiva [10].

Reconocimiento de la geometría de la mano:
La mano tiene aproximadamente 96 características por las cuales se puede diferenciar a una persona como por ejemplo el ancho de la palma de la mano, la longitud de los dedos, la distancia entre los dedos, la distancia entre nudillos, etc.
La técnica es útil para la verificación de identidad pero no es lo suficientemente confiable para la identificación [11].
Si bien las manos se mantienen invariantes a lo largo de la vida de una persona, pueden sufrir variaciones debido a cambios ambientales o naturales.

Reconocimiento por huellas digitales:
Se extraen características desde distintos ángulos y sectores del dedo y se almacenan. Las huellas dactilares son inalterables a lo largo de la vida de una persona pero lastimaduras, humedad, cicatrices o suciedad pueden alterarlas.
Se trata de una de las tecnologías más empleadas y en las que se han desarrollado diferentes dispositivos de bajo costo que permiten generalizar su aplicación [12] [13] [14].

Reconocimiento por firmas:
Se utiliza para verificar la identidad de las personas midiendo las características de escritura de su firma.
Al realizar una firma la persona ejecuta una serie de movimientos que contienen una información biométrica única, como el ritmo personal, la aceleración y la presión.
Se trata de una técnica muy difundida que en algunas ocasiones se combina con el encriptado de datos, para obtener mayor seguridad en operaciones sobre InterNet. De hecho muchos países han adoptado legislaciones relacionadas con firma digital, enfocando la utilización de esta técnica básica.

Reconocimiento por voz:
Una persona realiza una combinación de factores fisiológicos al hablar que resultan únicos de cada persona.
Este tipo de reconocimiento utiliza estas características para determinar la identificación de una persona, para lo cual se requiere un proceso de "aprendizaje" para determinar su patrón de voz, en el cual se digitaliza la expresión de los fonemas básicos y se genera un patrón o "template" para futuras comparaciones [15].

2. Análisis de la utilización de la técnica de huellas dactilares

La elección de la técnica a utilizar no es una tarea trivial, ya que algunas son netamente invasivas y pueden ser rechazadas por los usuarios/empleados.
Cada método biométrico mencionado anteriormente tiene sus ventajas y desventajas, según la aplicación que se haga de él y las personas que utilicen los equipos. Ningún método es infalible. Aparte de la precisión y la seguridad de los equipos biométricos, hay que considerar también otros factores, como la facilidad de uso, la aceptación por parte del usuario, el mantenimiento y el costo.
El reconocimiento mediante huellas digitales tiene algunas ventajas sobre otras técnicas biométricas, fundamentalmente porque la tecnología de implementación es más simple, notoriamente más barata y las huellas además son imborrables, cuantificables y únicas.

Las huellas digitales son características exclusivas de los primates.
En la especie humana se forman a partir de la sexta semana de vida intrauterina y no varían en sus características a lo largo de toda la vida del individuo. Son las formas que adopta la piel que cubre las yemas de los dedos.
Están constituidas por líneas que forman salientes y depresiones. Las salientes se denominan crestas papilares y las depresiones surcos interpapilares. En las crestas se encuentran las glándulas sudoríparas. El sudor que éstas producen contiene aceite, que se retiene en los surcos de la huella, de tal manera que cuando el dedo hace contacto con una superficie, queda un residuo de ésta, lo cual produce un facsímil o negativo de la huella.
Cada persona en el mundo tiene sus propias huellas digitales, diferentes a las de cualquier otra persona. Son diferentes en cada dedo en ambas manos e incluso entre gemelos idénticos.
Pero aunque cada uno tiene huellas digitales únicas, hay patrones básicos que siempre se encuentran y ayudan a clasificar las huellas digitales: en un dedo aparecen 7 puntos característicos que se repiten indistintamente para formar entre 60 y 120 puntos. A estos puntos se les llaman minucias, término utilizado en la medicina forense que significa "punto característico".
Además de las minucias, las huellas dactilares contienen dos tipos especiales de rasgos llamados puntos *core* y *delta*. Estos puntos son referidos como los puntos de singularidad de una huella dactilar.
El punto *core* es definido como el punto más alto en la línea curva más interior. Este punto es generalmente usado como punto de referencia para la codificación de minucias. El delta es el punto donde las líneas se dividen o se apartan.

Todas las características mencionadas permiten una digitalización y representación simbólica reducida de la imagen de la huella digital, con muy buena confiabilidad para su identificación sin necesidad de hacer una comparación "píxel a píxel" de las representaciones digitales [17].

3. Verificación de identidad en sistemas de E-Government

Es el interés de los gobiernos avanzar en la modernización de sus sistemas de información llevando sistemas centralizados a sistemas que pueden ser utilizados a través de la Web, ya que esta migración agilizará la utilización de los mismos y permitirá un mayor control y auditabilidad.

En general la utilización de tecnología para el acceso del ciudadano a los servicios propios de la gestión (Municipal, Provincial o Nacional) así como los mecanismos que permiten la participación directa del ciudadano en la toma de decisiones (o en la formación de opinión para la toma de decisiones) se denomina "Gobierno electrónico" o E-Government.

Estos mecanismos de inclusión digital del ciudadano requieren la verificación de las personas que tienen acceso a información de carácter sensible o que están habilitadas para la realización de operaciones concretas (expedientes, solicitudes, votaciones).

En general el grado de seguridad requerido alientan el empleo creciente de técnicas biométricas de reconocimiento. En particular al migrar aplicaciones a sistemas Web se hace crítico el empleo de técnicas (y tecnologías) confiables para el acceso a las funcionalidades que se soliciten.

Si bien no es excluyente, el empleo de técnicas de reconocimiento biométrico como las huellas digitales prometen dar respuesta en numerosos casos de E-government. Este proceso está acompañado de una disminución de los costos de los equipos y un incremento en la accesibilidad a los sistemas de comunicación de alta velocidad en las ciudades [18].

4. Caso de Estudio

Se presenta el análisis de cuatro casos en los que existe la necesidad de validación de la identificación de la persona mediante el reconocimiento de huellas dactilares: acceso a archivos confidenciales, emisión de sufragios, modificación de documentación crítica y obtención de certificados de supervivencia en el cobro de pensiones y jubilaciones

Acceso a archivos confidenciales: la protección de archivos, restringiendo el conocimiento del contenido de los mismos a sólo un grupo de usuarios autorizados, plantea un problema de seguridad que puede ser resuelto a través de la identificación del usuario por sus huellas dactilares. Estos usuarios sólo deben posar el dedo sobre el scanner de huellas dactilares para restaurar el contenido del archivo protegido. Al proteger un archivo se debe indicar qué usuarios pueden tener acceso, los cuales fueron dados de alta previamente en la base de datos junto con sus huellas digitales. El sistema crea un nuevo archivo encriptado conteniendo las huellas de los usuarios seleccionados y el contenido del archivo origen. Para desproteger un archivo, se debe posar el dedo sobre el scanner. Si el archivo contiene la huella del usuario, se desencripta el contenido del archivo origen.

Emisión de sufragios: actualmente los electores se presentan en las mesas de votación con su DNI y el presidente de mesa constata la foto del documento con la de la persona que lo presenta, en muchos casos el DNI está en mal estado o la foto no es clara, quedando la decisión final a criterio del presidente de mesa. Una opción para lograr una verificación de identidad precisa, es la utilización de una técnica biométrica. El reconocimiento por huellas dactilares parece ser lo más adecuado ya que se trata de una técnica sencilla, eficiente, de reconocimiento rápido y poco

invasiva. Para utilizar esta técnica en Urnas Electrónicas que incluyan una Terminal de Autoridades desde donde se verifica la identidad, se puede adicionar el sensor de huellas dactilares a la Terminal para que luego que el presidente de mesa ingrese el DNI del elector, le solicite al mismo que coloque su dedo pulgar derecho sobre el sensor, de esta manera el sistema podrá comparar las muestras obtenidas del sensor con la información asociada al DNI de la persona, pudiendo verificar su identidad. Es posible evitar el ingreso del DNI y que el sistema identifique directamente a la persona a través de sus huellas dactilares, pero esta tarea demoraría más tiempo ya que tendría que comparar la muestra contra todas las muestras de las personas del padrón. El proceso de verificación de electores puede también utilizarse independientemente de la urna electrónica, realizándose el proceso electoral de forma manual.
La flexibilidad de las comunicaciones ha llevado a que las personas puedan realizar reuniones a distancia, pero cuando llega el momento de tomar decisiones críticas, que requieren de una votación, debe garantizarse que quien se encuentre del otro lado de la comunicación sea quien dice ser. Actualmente este tipo de reuniones puede realizarse con diferentes tipos de herramienta sobre Internet donde basta con que la persona que tiene que votar coloque su dígito pulgar sobre el sensor conectado a la computadora o utilice un mouse con lector de huellas digitales para validar su identidad. La información obtenida por el sensor es cifrada bajo métodos de encriptación de clave pública/privada y transmitida hacia el centro de la comunicación donde es recibida, desencriptada y comparada con la información de la persona para verificar su identidad. Este procedimiento puede aplicarse para las votaciones a distancia.

Modificación de documentación crítica: es muy común que las personas trabajen desde diferentes municipalidades, organismos públicos, dependencias, etc., utilizando información centralizada en la Web o en servidores compartidos de acceso remoto. La información allí disponible puede ser de carácter crítica y la modificación de los documentos es un problema, ya que los usuarios de esa información podrían llegar a tomar decisiones erróneas. La tarea de modificar y publicar la información debe realizarse por personas autorizadas. En los casos que la información sea de carácter crítica, es posible la utilización de dispositivos de captura de huellas dactilares para verificar la identidad de la persona que está realizando la modificación.

Obtención de certificados de supervivencia: en la actualidad los jubilados y pensionados que cuentan con apoderados o residen en el exterior, para poder percibir sus haberes periódicamente tienen que presentar un certificado de supervivencia, el cual consiste en que se dirijan a un departamento de policía con su documento y un oficial emita dicho certificado que luego el apoderado presenta ante el ente solicitante. Este trámite podría realizarse a través de un sistema WEB que permita la identificación del interesado por huellas dactilares.

5. El problema de la confiabilidad y el tiempo de respuesta en sistemas Web con identificación biométrica basada en huellas digitales.

La aplicación del reconocimiento de huellas digitales a casos de gobierno electrónico como los mencionados en el punto anterior tiene algunas dificultades concretas, entre las cuales se puede mencionar:

- Normalmente la Base de Datos de usuarios (y por ende de huellas digitales) crece y el problema de su acceso en tiempos razonables escala en forma no necesariamente lineal.

Esto requiere una optimización de los algoritmos de digitalización, representación y reconocimiento de los patrones de la huella, de modo de poder manejar el crecimiento del número de usuarios o bien hacer portable la aplicación, por ejemplo de una ciudad de 10.000 habitantes a otra de 500.000 habitantes.
De hecho entre las soluciones está también la paralelización de los algoritmos de identificación y/o la distribución física de los datos a reconocer, de modo de minimizar el espacio de búsqueda.
En este trabajo se ha realizado experimentación con tamaños de BD desde 300 a 100.000 huellas.

- Las comunicaciones en las aplicaciones de E-Government son un factor crítico. Dado que normalmente lo que podemos esperar de usuarios en una ciudad (o en un área geográfica que abarque varias ciudades) es que tengan conexiones a InterNet de diferente capacidad y considerando que la respuesta de la red WAN que da acceso a los servicios depende de un tráfico que normalmente es muy variable (fundamentalmente cambia con el día y la hora de utilización), modelizar las aplicaciones para asegurar un tiempo de respuesta es muy difícil.
  Más aún, clases de aplicaciones que requieren respuestas en tiempo real desde puntos geográficamente dispersos (por ejemplo voto electrónico con identificación por la huella digital) pueden resultar críticas si no se estiman adecuadamente las condiciones de "caso peor" o si existen fallas en los mecanismos de digitalización previa o en el momento de la operación.

- Por último hay que mencionar que el grado de confianza requerido depende de la clase de aplicación. Una consulta popular no vinculante puede admitir márgenes de error en el reconocimiento seguro de los usuarios mayor que una certificación de una transacción financiera o el registro de una escritura pública. Por esto es necesario estudiar la tecnología a emplear, en el contexto real y analizar detalladamente las posibles causas de falla o error.
  En nuestro caso se estudiaron condiciones de pérdida o alteración de las huellas, para medir el efecto en la identificación efectiva del usuario.

6. Trabajo experimental realizado

Se utilizó un scanner modelo "fs80 de Futronic" de huellas dactilares con sensores de tecnología cmos y un sistema óptico preciso para entregar una imagen de alta calidad de la huella digital. La huella dactilar es iluminada por 4 leds infrarrojos cuya intensidad se ajusta automáticamente a las características de la huella, es decir la intensidad varía si la huella esta húmeda o borrosa por ejemplo.

Para el reconocimiento se utilizó una serie de librerías denominadas VeriFinger. Se trata de un motor de identificación de huellas dactilares diseñado para aplicaciones biométricas concretas. Permite ser utilizado en verificación 1:1 o reconocimiento 1:n, el algoritmo de reconocimiento de huellas utiliza un esquema de identificación a partir de un conjunto de puntos específicos de la huella denominado minucia. Además es tolerante a traslación y rotación de las imágenes de huellas. Utiliza un algoritmo original que permite comparar 30000 huellas por segundo e identificar huellas aún si están rotadas, o trasladadas con sólo 5 a 7 minucias similares (usualmente dos huellas del mismo dedo contienen 20 a 40 minucias similares). No requiere la presencia del centro o delta de la huella en la imagen, y puede reconocer una huella a partir de cualquier parte de la misma. De todas maneras si estas características están presentes, la utiliza para un reconocimiento más confiable. La base de datos está preordenada utilizando ciertas características globales. La comparación es

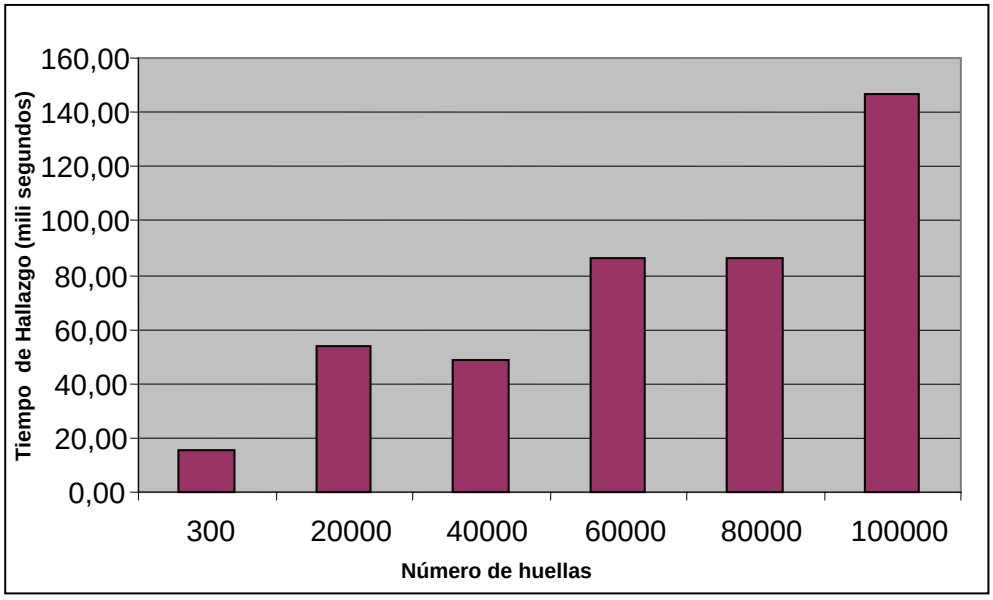
realizada primero contra las huellas almacenadas que contienen similares características globales a la que se está evaluando. Si la comparación contra este grupo no arroja resultados positivos, el próximo registro con características globales similares es seleccionado, y así continúa hasta que el reconocimiento es positivo o hasta que se llega al final de la base de datos. En la mayoría de los casos hay una alta probabilidad de que el reconocimiento exitoso se alcance al comienzo de la búsqueda. Como resultado, la cantidad de comparaciones requeridas para alcanzar un reconocimiento exitoso decrece drásticamente, y consecuentemente, la velocidad de respuesta efectiva es mayor. Enrola por generalización de características a partir de tres imágenes de la misma huella. Cada imagen es procesada y sus características son extraídas. Luego las tres colecciones de características son analizadas y combinadas en una sola colección de características combinadas, que es la que se escribe en la base de datos. De esta manera la minucia enrolada es más confiable y la calidad y confiabilidad del reconocimiento son incrementadas.

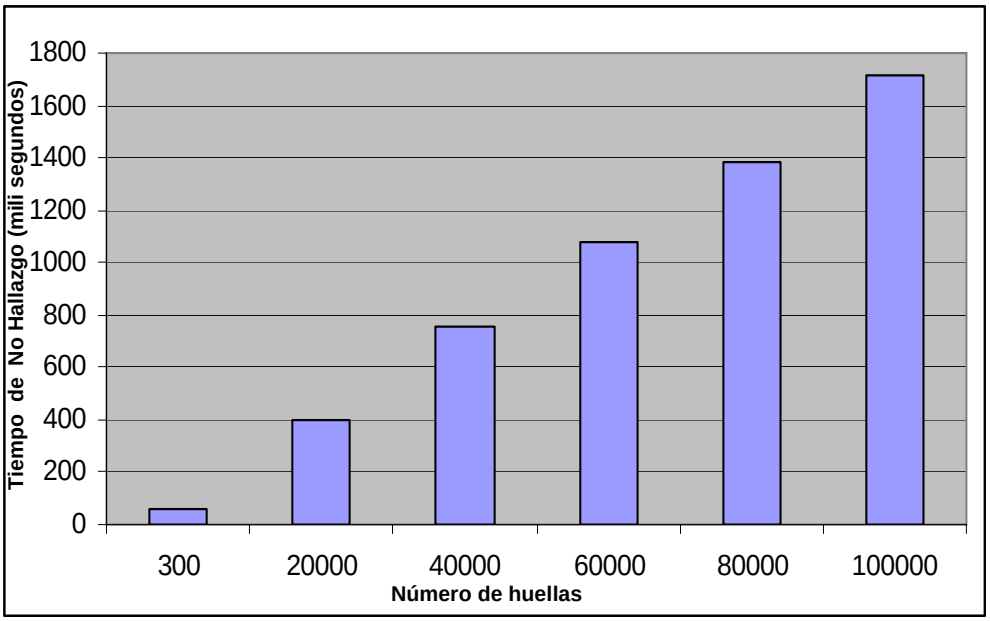
Escalabilidad de los tiempos de respuesta según el volumen de la base de datos

Se almacenaron alrededor de 300 huellas dactilares, luego se replicaron en la base hasta llegar a los 20000, 40000, 60000, 80000, 100000, a las copias se les introdujeron alteraciones para garantizar que en el proceso de identificación las huellas sean únicas.

En la tabla y gráficos presentados se analizan los tiempos de respuesta en el reconocimiento con la BD creciente.

Cantidad de huellas	Tiempo de hallazgo (mili segundos)	Tiempo de no hallazgo (mili segundos)
300	15,16	59
20000	53,79	399
40000	48,91	756
60000	86,42	1076
80000	86,51	1384
100000	146,89	1711





Análisis de alteraciones en la adquisición de la huella dactilar

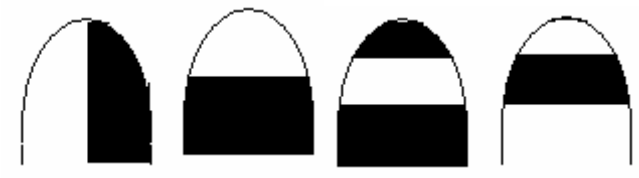
Se simularon una serie de alteraciones que pueden ocurrir en el proceso de adquisición de la huella.

- Alteraciones en la digitalización

Se simuló suciedad en la ventana de adquisición del scanner cubriéndola con cinta adhesiva transparente, hasta dos capas funcionó correctamente, luego la calidad de la huella no fue suficiente para la identificación ya que en la imagen se identificaban claramente los límites de la cinta adhesiva que fueron tomados como posibles minucias de la huella a buscar.
Se intentó realizar una identificación a bajas temperaturas, es decir la huella dactilar por alrededor de los cero grados y el scanner no adquirió la huella.

- Alteraciones de las yemas de los dedos

Se cubrió la yema del dedo con marcador de tinta indeleble como se ve en la figura y la huella no fue identificada, luego se realizó la misma prueba con marcadores al agua y se verificó la identificación en los cuatro casos.



Cubriendo la yema del dedo con cinta adhesiva transparente de la misma forma que indica la figura, las huellas fueron reconocidas en todos los casos.

7. Conclusiones y líneas de trabajo futuro

Se ha analizado la utilización de reconocimiento biométrico (en particular huellas digitales) en aplicaciones de E-Government, poniendo énfasis en los tiempos de respuesta para considerar la escalabilidad de las aplicaciones con el número de usuarios.
Se han estudiado casos de pérdida de información y su efecto sobre el porcentaje de identificación positiva de usuarios, de modo de considerar la confiabilidad de los procesos en función de la posible degradación de la información digitalizada.
Actualmente se trabaja analizando la dependencia del tiempo de respuesta según las características de los links de comunicación y la dinámica del tráfico sobre los mismos (sobre todo enfocado a InterNet).
También se estudia la paralelización y eventual distribución de la Base de Datos de huellas para mejorar los tiempos de respuesta, según la clase de aplicación de E-Government de interés.

8. Bibliografía

[1] Caballero Sybil Lorena. "Prácticas emergentes: la ciberdemocracia, las telecomunidades de conocimiento y los telecentros como alternativas para el desarrollo". CDC, jan. 2005, vol. 22, no. 58, p.97-114. ISSN 1012-2508.
[2] Brunet C., De Lafontaine J. y Schilling K. "Tele-Education in Engineering Using a Virtual International Laboratory". Innovations 2003 – World Innovations in Engineering Education and Research. 2003.
[3] Cabello R. y otros. "EMERGE: A European Educational Network for Dissemination of Online Laboratory Experiments". Innovations 2004 – World Innovations in Engineering Education and Research. 2004.
[4] Reid Paul. "Biometrics for Network Security". Prentice Hall 2004.
[5] Chirillo John y otros. "Implementing Biometric Security". Wiley Publishing 2003.
[6] Woodward J.D. Jr. y otros. "Biometrics". McGraw-Hill Osborne Media.
[7] Liu Simon and Silverman Mark. "A Practical Guide to Biometric Security Technology". IEEE Computer Society, IT Pro – Security.
[8] Biometric Consortium. http://www.biometrics.org/.
[9] International Biometrical Group. http://www.biometricgroup.com/.
[10] Areitio Javier, Areitio Teresa. "Análisis en torno a la tecnología biométrica para los sistemas electrónicos de identificación y autenticación". http://www.redeweb.com/_txt/630/52.pdf
[11] "Information Security - Challenges in Using Biometrics". Statement of Keith A Rhodes Chief Technologist Applied Research and Methods. http://www.gao.gov/new.items/d031137t.pdf
[12] Arsaute Gabriel Adrián, Tutores: Nasisi Óscar Herminio, Martín Marcelo. "Reconocimiento de características en huellas dactilares para la identificación humana". Universidad Nacional de San Juan. Facultad de Ingeniería. Instituto de Automática. 1997
[13] Beavan Colin. "Huellas dactilares. Los orígenes de la dactiloscopía". Ed. Alba. 1990.
[14] Arrieta Angélica, Marín José, Sánchez Luis García, Romero Luis, Sánchez Lázaro Ángel, Batista Vivian. "Gestión y Reconocimiento Óptico de los Puntos Característicos de Imágenes de Huellas Dactilares". Universidad de Salamanca.
[15] Grasso M, Finin Tim. "Integración de tareas en ambientes de reconocimiento de voz multimodales". 1999
[16] Jain L. C., Halici U., Hayashi I., Lee S. B.. "Intelligent biometric techniques in fingerprint and face recognition". 1999.
[17] Lee H. C., Gaensslen R. E. "Advances in fingerprint technology". 1994
[18] Srinivasan V. S., Murthy N. N. "Detection of singularity point in fingerprint images. Pattern Recognition". Vol 25, pp. 139-153. 1992.